



General Motors Company
25 Massachusetts Avenue, N.W.
Suite 400
Washington, D.C. 20001
Phone: 202-775-5080
Fax: 202-775-5023

October 7, 2016

Marlene H. Dortch
Secretary
Federal Communications Commission
445 Twelfth Street, SW
Washington, DC 20554

Re: Petition for Rulemaking and Request for Emergency Stay of Operation of Dedicated Short-Range Communications Service in the 5.850-5.925 GHz Band (5.9 GHz Band); RM 11771 (Petition)

Dear Ms. Dortch:

On behalf of General Motors Company (GM), this *ex parte* notice memorializes a meeting between representatives of GM and Chairman Wheeler's staff. On Thursday, October 6, 2016, Jeff Massimilla, Chief Product Cybersecurity Officer; Andrew York, Executive Director of Federal Affairs; and Richard Lopez, Director of Federal Affairs, met with Louisa Terrell, Advisor, and Edward Smith, Legal Advisor, Wireless, Engineering and Technology, Consumer Affairs and Incentive Auction of the office of Chairman Tom Wheeler. The purpose of the meeting was to discuss broadly the numerous actions GM has taken and continues to take to secure vehicle architecture, telematics, and the connected vehicle ecosystem from cybersecurity vulnerabilities and to further discuss GM's efforts and experience working with others in the automotive industry on these topics.

Mr. Massimilla gave a lengthy overview of the actions GM takes in carrying out the mission of the Product Cybersecurity organization. They include:

- security by design for GM products from the earliest days of development throughout the manufacturing process;
- defense in depth strategies with multiple layers of defenses presented to attack surfaces of cyber critical systems;
- rapid response to vulnerabilities via over the air updates as well as the ability to cut communications for specific groups of vehicles or to the entire fleet in a matter of seconds;

- work with security researchers, including the GM Security Vulnerability Disclosure Program, through which security researchers can inform GM of bugs or vulnerabilities via a secure website portal;
- vendor and supply chain management, including engaging with suppliers to provide education and training on how to minimize risk; and
- external collaboration with experts in the defense and aerospace industries, government organizations, academia and industry consortiums on best practices and key learnings: and

Mr. Massimilla also described the recently created Automotive Information Sharing and Analysis Center (Auto ISAC), of which Mr. Massimilla is the current Vice Chair. The Auto ISAC was created for Original Equipment Manufacturers and suppliers as an industry-operated environment created to enhance cyber security awareness and coordination across the global automotive industry. He explained that the Auto ISAC to date has been successful because of the cooperative engagement by all members to share threat and vulnerability information and to work together as an industry on cyber threat awareness and best practices. In July, the Auto ISAC released an Executive Summary identifying cybersecurity “best practices” for the auto industry that builds upon the Proactive Safety Principles agreed to by the auto industry and the Department of Transportation. Mr. Massimilla explained that GM supported and endorsed all recommendations in the Executive Summary and committed to implementing the actions and best practices outlined in the document. Mr. Massimilla also explained that they have expanded the ISAC to include the telecommunications and trucking industries to address cybersecurity threats and vulnerabilities across all levels of the transportation industry.

In response to questioning, Mr. Massimilla explained that Dedicated Short Range Communications (DSRC) systems are an additional connected ecosystem that were developed with a Security Credential Management System (SCMS) in place and separated from safety critical and infotainment systems. The SCMS system ensures the protection of communications between vehicles (V2V), vehicles to infrastructure (V2I), and vehicles to pedestrians (V2P). He discussed how revocation adds to security. If a bad certificate is found within the system it is ignored and locked out so that the infected communication does not spread to other vehicles or infrastructure.

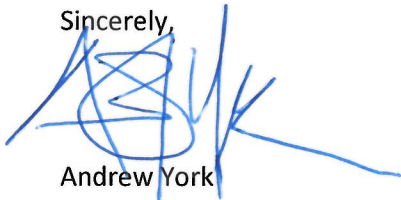
Mr. Massimilla also cautioned the Commission that prescriptive rules and regulations that would be potentially outdated by the time they were published could actually hinder cybersecurity rather than enhance it. Instead, he stressed an emphasis on risk management and cross industry and governmental collaboration as an appropriate approach to cybersecurity. He noted the interaction between GM, the auto industry, and the National Highway Traffic Safety Administration (NHTSA). He stressed that NHTSA, as a safety regulator of the auto industry, is developing guidance in cybersecurity and is in regular communication with OEM’s regarding cybersecurity topics.

Mr. York noted that NHTSA interprets its authority to include cybersecurity–related safety of motor vehicles and equipment and that a safety recall due to cybersecurity vulnerabilities has already occurred. Furthermore, he stressed that OEM’s have a statutory obligation to report any defect in vehicles affecting safety, including those due to cybersecurity vulnerabilities. In addition, the Federal Trade Commission (FTC) has used its authority under Section 5 of the FTC Act to exercise oversight of

cybersecurity incidents affecting privacy. Because of the comprehensive nature of regulatory oversight that already exists, he pointed out that additional regulations and oversight by the Commission was unnecessary.

This letter is being filed electronically pursuant to Section 1.1206 of the Commission's rules. Should you have any questions, please contact the undersigned.

Sincerely,

A handwritten signature in blue ink, appearing to be 'Andrew York', with a stylized, overlapping loop structure.

Andrew York
Executive Director, Federal Affairs